

МОТИВОВАНИЙ ВИСНОВОК ЩОДО ВНЕСЕННЯ ЗМІН ДО ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «КІБЕРБЕЗПЕКА»

Відповідно до п.5 «Тимчасового порядку розроблення, затвердження, моніторингу та періодичного перегляду освітніх програм у ДВНЗ «Донецький національний технічний університет», затвердженого Наказом ДВНЗ «ДонНТУ» від 12.04.2021 р. №158, в зв'язку з внесенням змін до стандарту вищої освіти зі спеціальності 125 «Кібербезпека» (наказ МОН від 29.10.24 №1547), із змінами в групі забезпечення ОПП та заміною гаранта спеціальності, та з огляду на необхідність періодичного перегляду ОПП вважаємо за доцільне внести зміни до освітньо-професійної програми «Кібербезпека та захист інформації» ОС «Бакалавр» спеціальності «Кібербезпека та захист інформації».

З огляду на швидкоплинність змін у галузі знань кібербезпеки, важливо актуалізувати зміст дисциплін програми для забезпечення відповідності загальним та спеціальним (фаховим) компетентностям, а також результатам навчання. Відновлення періодичності перегляду освітньо-професійної програми дозволить врахувати новітні тенденції та виклики у сфері кібербезпеки, у т. ч. пов'язані з безпекою критичних інфраструктур (Закон України "Про критичну інфраструктуру" (№ 1882-IX), що є критично важливим для підготовки кваліфікованих фахівців та майбутньої акредитації спеціальності.

Актуалізація освітньо-професійної програми сприятиме підвищенню якості освітнього процесу, забезпечуючи відповідність програми сучасним вимогам, які висуваються Національним агентством із забезпечення якості вищої освіти під час акредитації освітніх програм.

Гарант ОПП

Ярослав ДОРОГИЙ

Зав. кафедри ПМІ

Наталія МАСЛОВА

Висновок розглянуто та схвалено на засіданні кафедри прикладної математики та інформатики 15 листопада 2024 р. (протокол №11)

Перелік змін до Освітньо-професійної програми
«Кібербезпека»

Стор.	Зміни/сутність змін – 2024р	Дані 2020р.
	Титул. Заміна (очищення) граф дат, прізвищ, підписів	
1	Бакалавр з кібербезпеки	Фахівець із організації інформаційної безпеки
1	Дрогобич - 2024	Покровськ-2020
2	Лист погодження – заміна підписувачів, дат та протоколів узгодження	
4	Передмова – змінено анонс, робочу групу, терміни	
5	Профіль освітньої програми – уточнення й коригування дат в п.п. 1.1,	
6	Класифікатор професій, а саме: 2139.2. Адміністратор безпеки мереж і систем 2139.2. Фахівець сфери захисту інформації 2139.2. Фахівець з питань безпеки (інформаційно-комунікаційні технології) 2139.2. Конструктор систем кібербезпеки 2139.2. Фахівець з підтримки інфраструктури кіберзахисту 2139.2. Фахівець з реагування на інциденти кібербезпеки 2139.2. Фахівець з криптографічного захисту інформації 2139.2. Фахівець з технічного захисту інформації 2139.2. Фахівець з тестування систем захисту інформації 2139.2. Аудитор інформаційних технологій (з кібербезпеки) 2139.2. Фахівець з оцінки заходів захисту інформації (кібербезпеки)	Класифікатор професій, а саме: 3439. Фахівець з організації інформаційної безпеки 3121. Фахівець з інформаційних технологій
7	<u>1.6 Перелік компетентностей випускника</u> <u>Загальні компетентності</u> ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.	<u>1.6 – Програмні компетентності</u> <u>Загальні компетентності (ЗК)</u> ЗК02. Знання та розуміння предметної області та розуміння професії. ЗК03. Здатність спілкуватися рідною та іноземною мовами як усно, так і письмово

	<p>ЗК4. Здатність спілкуватися іноземною мовою.</p> <p>ЗК5. Здатність вчитися і оволодівати сучасними знаннями.</p> <p>ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>ЗК7. Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.</p> <p>ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.</p>	<p>ЗК04. Вміння виявляти, ставили та вирішувати проблеми за професійним спрямуванням</p> <p>ЗК05. Здатність до пошуку, оброблення та аналізу інформації.</p> <p>ЗК06. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства, необхідність його сталого розвитку, верховенства права, прав і свобод людини, громадянина в Україні;</p> <p>ЗК07. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форм рухової активності для активного відпочинку та ведення здорового способу життя,</p>
7-8	<p><u>Спеціальні (Фахові, предметні) компетенції</u></p> <p>ФК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та Міжнародні вимоги, практики і стандарти у професійній діяльності.</p> <p>ФК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.</p> <p>ФК 3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.</p> <p>ФК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.</p> <p>ФК 5. Здатність відновлювати функціонування інформаційних, інформаційно-комунікаційних систем після</p>	<p><u>Фахові компетентності спеціальності (ФК)</u></p> <p>ФК01. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та Міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки</p> <p>ФК02. Здатність до використання інформаційно- комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки</p> <p>ФК03. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах</p> <p>ФК04. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК05. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p>

		<p>реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.</p> <p>ФК 6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)</p> <p>ФК 7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.</p> <p>ФК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>ФК 9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>ФК 10. Здатність виконувати моніторинг інформаційних, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.</p>	<p>ФК06. Здатність відновлювати штатне. Функціонування інформаційних, ' інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження.</p> <p>ФК07. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)</p> <p>ФК08. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p> <p>ФК09. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.</p> <p>ФК10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p> <p>ФК11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно- телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.</p> <p>ФК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки</p>
8	1.7 Нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання		1.7 - Програмні результати навчання
8-9	ПРН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.		ПРН01. Застосувати концептуальні знання з навчальних дисциплін загальної підготовки для засвоєння навчальних дисциплін професійної підготовки;
	ПРН 2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.		ПРН02. Організувати власну професійну діяльність, обирати та способи розв'язування складних спеціалізованих задач та практичних проблеми професійній діяльності, оцінювати їхню ефективність;
	ПРН 3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.		ПРН03. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

	ПРН 4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.	ПРН04. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;
	ПРН 5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.	ПРН05. Адаптуватися в умовах часткої зміни технологій професійної діяльності, прогнозувати кінцевий результат;
	ПРН 6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.	ПРН06. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності
	ПРН 7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.	ПРН07. Діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та/або кібербезпеки;
	ПРН 8. Застосовувати знання і розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.	ПРН08. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки;
	ПРН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.	ПРН09. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;
	ПРН 10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.	ПРН10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;
	ПРН 11. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.	ПРН11. Виконувати аналіз зав'язків Між інформаційними процесами на віддалених обчислювальних системах;

	ПРН 12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.	ПРН12. Розробляти моделі загроз та порушника;
	ПРН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.	ПРН13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандарт. технологіях та протоколах передачі даних;
	ПРН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.	ПРН14. Вирішувати завдання захисту програм та інформації, що обробляється В інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;
	ПРН 15. Збирати, обробляти зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводили аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.	ПРН15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;
	ПРН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	ПРН16. Реалізовувати комплексні системи захисту інформації В автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;
	ПРН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.	ПРН17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;
	ПРН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.	ПРН18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

	ПРН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.	ПРН19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації" в інформаційно-телекомунікаційних системах;
	ПРН 20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.	ПРН20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;
	ПРН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дії з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	ПРН21. Вирішувати задачі забезпечення та супроводу (в .т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки В інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
		ПРН22. Вирішувати задачі управління процедурами ідентифікації, автентифікації', авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і/або кібербезпеки;
		ПРН23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів В інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
		ПРН24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);
		ПРН25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;
		ПРН26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту

		інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем;
		ПРН27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;
		ПРН28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки;
		ПРН29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;
		ПРН30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
		ПРН31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;
		ПРН32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;
		ПРН33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;
		ПРН34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;
		ПРН35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки;
		ПРН36. Виявляти небезпечні сигнали технічних засобів;
		ПРН37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та

			визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;
			ПРН38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;
			ПРН39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;
			ПРН40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;
			ПРН41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;
			ПРН42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;
			ПРН43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів;
			ПРН44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;
			ПРН45. Застосовувати ріні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
			ПРН46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;

			ПРН47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;
			ПРН48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;
			ПРН49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;
			ПРН50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);
			ПРН51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;
			ПРН52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;
			ПРН53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
			ПРН54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
	11	ВБ 1.5 Кібербезпека критичних інфраструктур	ВБ 1.5 Методи аналізу даних
	12	ВБ 2.5 Захист критичних інфраструктур	ВБ 2.5 Емпіричні методи кібербезпеки
	15	В матрицю відповідності програмних компетентностей компонентам освітньої програми додано рядок інтегральних компетентностей	